Nattan MAISONNEUVE–FLEURY
BTS SIO 1
Groupe B

09/10//2025

Compte Rendu - Donnée hachée et volée

Sommaire :

Introduction :

Dans ce TP nous allons voir comment fonctionne un serveur NAS et comprendre pourquoi c'est important et utile d'en avoir un, surtout dans les entreprises.

Partie 1 :

Etape 1 :

Premièrement on créer une dossier bloc-note avec du texte dedans, par exemple :
C'est un fichier texte qui va être utilisé pour vérifier l'intégrité des données

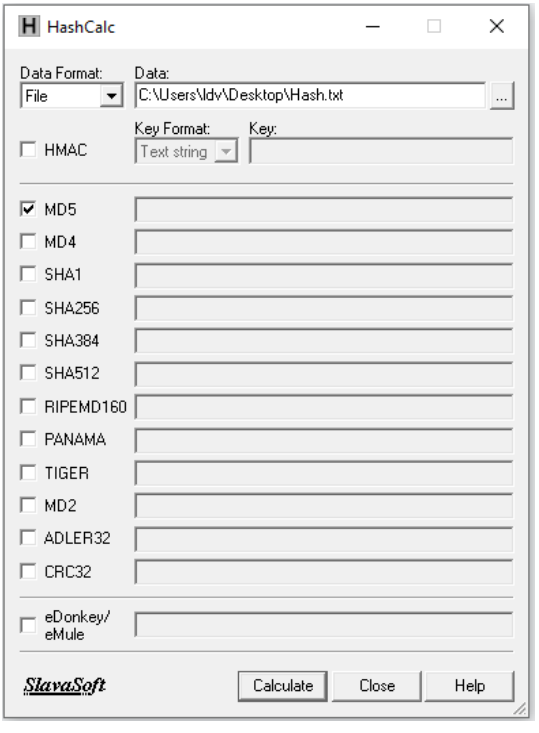
Ensuite, on enregistre en mettant le nom **Hash.txt.** On met le fichier sur le bureau pour le retrouver plus facilement.

Etape 2 :

Maintenant on installe le logiciel de Hash depuis ce lien :
https://hashcalc.software.informer.com/download/

Etape 3 :

On configure maintenant le logiciel comme ceci :



On peut maintenant appuyer sur calculate et nous avons ce résultat :
MD5 = 2bedcf8c84727e946e8eb13a643529e2

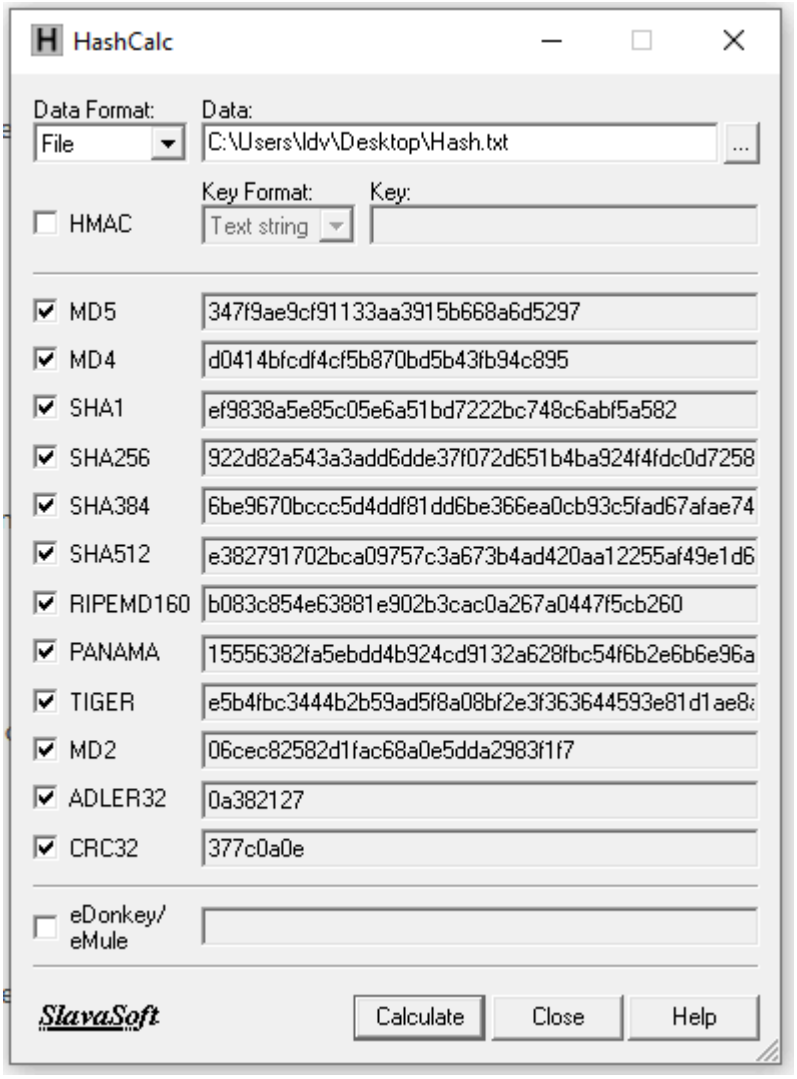
Etape 4 :

On peut modifier le texte dans Hash.txt afin de voir si le code numéro change. On peut par exemple rajouter une lettre :
C'est un fichier texte qui vas être utilisé pour vérifier l'intégrité des données

Etape 5 :

On peut recalculer et nous avons ce résultat :
MD5 = 347f9ae9cf91133aa3915b668a6d5297

Pour voir tous les hash on peut tout cocher comme ceci :



La taille d'un Hash change selon le mode (MD5, SHA, Adler…) parce que chaque algorithme produit une empreinte de longueur fixe différente, définie par sa conception.

Partie 2 :

Date de l'incident	**Entreprise touché**	**Nombres de victimes données volées**	**Méthodes utilisées Mesure(s) de protection prise(s)**	**Source de référent**
Juillet 2025	Qantas	~5+ millions de clients affectés	Accès via un fournisseur tiers / compromission de base de données ; social engineering rapporté. Enquête avec experts externes, injonction judiciaire pour limiter diffusion, renforcement des sécurités côté fournisseur et recommandations aux clients (surveillance, vigilance phishing).	https://www.reuters.com/sustainability/boards-policy-regulation/qantas-says-customer-data-released-by-cyber-criminals-months-after-cyber-breach-2025-10-12/
20 décembre 2023	First american financial	centaines de million	Accès non autorisé aux systèmes (exfiltration + chiffrement dans certains cas) — exploitation de systèmes non-productifs et vulnérabilités internes. Notifications, analyse forensique, chiffrement renforcé, procédures juridiques et actions correctives (selon dépôts SEC).	https://www.cybersecuritydive.com/news/first-american-44k-breached-cyberattack/717377/
Mai-Dec 2023	Progress MOVEit	~2 600 organisations et ~85–90 millions d'individus touchés	Exploitation d'une vulnérabilité zero-day dans le logiciel MOVEit par le gang Cl0p (exploitation MFT → exfiltration). Correctifs de Progress, patching urgent, audits des	https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/

			transferts de fichiers, rotations de credentials, notification des victimes. Beaucoup d'organisations ont engagé analyses forensiques et mesures d'atténuation.	
Dec 2024 - Jan 2025	Cleo	Des dizaines d'organisations	Compromission de la solution MFT (chaîne d'attaque sur l'écosystème fournisseurs) ; publication/exfiltration par le groupe Cl0p. Investigations, notifications, mesures correctives chez Cleo et chez clients, recommandations de rotations de clés et segmentation.	https://www.opswat.com/blog/lessons-from-the-cleo-exploit-evidence-underscores-why-secure-mft-is-critical
Aout - Septembre 2025	Miljödata	Données RH sensibles pour employés	Ransomware / accès non autorisé au fournisseur HR (compromission fournisseur SaaS/tiers). Forensic et containment, notification aux parties affectées, renforcement des contrôles fournisseurs, révision des SLA de sécurité.	https://www.securityweek.com/volvo-group-employee-data-stolen-in-ransomware-attack/

Pour éviter ce genre de problèmes il existe plusieurs méthodes :

- Mettre à jour régulièrement les logiciels
- Utiliser des mots de passe forts et la double authentification
- Former le personnel contre le phishing
- Chiffrer et sauvegarder les données importantes (hashage)
- Surveiller les accès et contrôle la sécurité des fournisseurs

Conclusion :

Dans ce TP nous avons vu comment Hasher des données et voir quels ont été les plus gros vols de données cette dernière année. La première partie du TP a été très simple et rapide et m'a permis de découvrir différentes formes de hash. La deuxième partie à été plus longue a cause du tableau et des nombreuses recherches qu'il fallait effectuer. Cependant cela nous a permis de découvrir plusieurs attaques et de voir que n'importe qui pouvait être touché.